

Amendments to the Claims:

The listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

- 5 1 (currently amended): A method for determining whether a
communication device is permitted to access communication service
in a communication network, the communication device comprising:
a data memory capable of storing ciphertext access information;
and
10 an inerasable memory capable of storing a deciphering key in a
non-volatile way; and
the method comprising:
enciphering access information corresponding to the
communication device into the ciphertext access
15 information using a predetermined cryptography
algorithm according to an enciphering key stored outside
of the communication device, wherein the enciphering
key corresponds to the deciphering key, and wherein the
communication network comprises a service provider capable of
20 providing communication service to the communication
device; there being a database in the service provider for
recording the enciphering key corresponding to the communication
device; and
recording the ciphertext access information in the data
25 memory;
reading the deciphering key in the inerasable memory and the
ciphertext access information in the data memory; and
deciphering the ciphertext access information to plaintext
access information according to the deciphering key by
30 using a ~~predetermined~~ the cryptography algorithm, and

determining whether the communication device is permitted to access communication service in the communication network accordingly.

5 2 (original): The method of claim 1 wherein the cryptography algorithm is an asymmetric encryption-and-decryption algorithm.

3 (original): The method of claim 1 wherein the data memory is a non-volatile memory.

10

4 (cancelled)

5 (currently amended): The method of ~~claim 4~~ claim 1 further comprising:
generating the enciphering key and the corresponding deciphering key
15 according to the cryptography algorithm before generating the ciphertext access information according to the enciphering key.

6 (cancelled)

20 7 (currently amended): The method of ~~claim 6~~ claim 1, wherein when generating the ciphertext access information according to the enciphering key, the service provider enciphers the access information corresponding to the communication device to generate the ciphertext access information according to the enciphering key stored in the database.

25

8 (original): The method of claim 7, wherein when recording the ciphertext access information in the data memory, transmitting the ciphertext access information from the service provider to the communication device via the communication network, and recording the ciphertext
30 access information in the data memory with the communication

device.

9 (currently amended): The method of ~~claim 4~~ claim 1, wherein the
enciphering key is different from the deciphering key.

5

10 (original): The method of claim 1, wherein when determining whether the
communication device is permitted to access communication service
of the communication network according to the plaintext access
information, determining whether the plaintext access information
10 conforms to predetermined access information; the communication
device being determined permitted to access the communication
service of the communication network if the plaintext access
information conforms to the predetermined access information.

15 11 (original): The method of claim 1 in which the communication device
further comprises a subscriber identification module card (SIM card)
capable of recording a subscriber identification number, and a
predetermined identification number is recorded in the plaintext
access information, wherein when determining whether the
20 communication device is permitted to access communication service
in the communication network according to the plaintext access
information, determining whether the subscriber identification code
conforms to the predetermined identification code; the
communication device being permitted to access the communication
25 service if the predetermined identification code and the subscriber
identification code correspond to each other, and the communication
device being not permitted to access the communication service and
having access to the communication network stopped if the
predetermined identification code and the subscriber identification
30 code do not correspond to each other.

12 (currently amended): A communication device utilized in a
communication network for accessing communication service of the
communication network; the communication device comprising:
5 a data memory capable of storing ciphertext access information in
a non-volatile way;
an inerasable memory capable of storing a deciphering key in a
non-volatile way; and
a processor capable of controlling operation of the communication device;
10 wherein before the communication device accesses the communication service of
the communication network, the processor reads the deciphering key in the
inerasable memory and the ciphertext access information in the data memory,
utilizes a predetermined cryptography algorithm to decipher the ciphertext access
information to plaintext access information according to the deciphering key, and
15 determines whether the communication device is permitted to access
communication service of the communication network according to plaintext
access information;
wherein the communication network comprises a service provider for providing
communication service to the communication device; there being a
20 database in the service provider capable of recording an enciphering key
corresponding to the communication device, the enciphering key being stored
outside of the communication device; the ciphertext access
information being generated by enciphering the access information
corresponding to the communication device by the cryptography
25 algorithm according to the enciphering key, wherein the enciphering
key corresponds to the deciphering key.

13 (original): The communication device of claim 12 wherein the
cryptography algorithm is an asymmetric
30 encryption-and-decryption algorithm.

14 (cancelled)

15 (currently amended): The communication device of ~~claim 14~~ claim 12
5 wherein the enciphering key and the corresponding deciphering key
 are generated according to the cryptography algorithm.

16 (currently amended): The communication device of ~~claim 14~~ claim 12
 wherein the ciphertext access information is transmitted from the
10 service provider to the communication device via the communication
 network, and recorded in the data memory by the communication
 device.

17 (original): The communication device of claim 12 wherein when the
15 processor determines whether the communication device is permitted
 to access communication service according to the plaintext access
 information, the processor determines whether the plaintext access
 information conforms to predetermined access information; wherein
 the processor determining the communication device is permitted to
20 access the communication service if the plaintext access information
 conforms to the predetermined access information.

18 (original): The communication device of claim 12 in which the
 communication device further comprises a SIM card capable of
25 recording a subscriber identification number, and a predetermined
 identification code is recorded in the plaintext access information,
 wherein when the processor determines whether the communication
 device is permitted to access communication service according to the
 plaintext access information, the processor determines whether the
30 subscriber identification code conforms to the predetermined

identification code; the communication device being permitted to
access the communication service if the predetermined identification
code and the subscriber identification code correspond to each other,
and the communication device being not permitted to access the
communication service and access to the communication network
being stopped if the predetermined identification code and the
subscriber identification code do not correspond to each other.

19 (original): The communication device of claim 12 in which the
communication device is a cell phone, and the communication
network is a wireless communication network.

20 (currently amended): A method applied in a communication network,
wherein the communication network comprises a plurality of
communication devices and each communication device comprises an inerasable
memory and a data memory; the method being capable of determining whether
each communication device is permitted to access communication service of the
communication network; the method comprising:

providing a plurality of different enciphering keys and a plurality of
deciphering keys according to a cryptography algorithm, wherein each
enciphering key corresponds to each deciphering key, wherein the
communication network further comprises a service provider capable of
transmitting signals and providing communication service among
communication devices, service provider having a database storing
enciphering keys corresponding to each communication device in the
database, the enciphering keys being stored outside of the
respective communication devices;

providing different corresponding enciphering keys to different
communication devices;
enciphering access information corresponding to each

communication device to ciphertext access information by
the cryptography algorithm according to the enciphering
key corresponding to the communication device;
storing deciphering keys corresponding to the enciphering keys
5 corresponding to each of the communication devices in the
inerasable memory;
storing ciphertext access information of each communication
device in the data memory of the communication device; and
when determining whether a communication device is permitted
10 to access the communication service, deciphering the
ciphertext access information in the data memory by the
cryptography algorithm according to the enciphering key
stored in the inerasable memory, and determining whether
the communication device is permitted to access the
15 communication service according to the deciphered
ciphertext access information.

21 (original): The method of claim 20, wherein the deciphering keys
corresponding to different enciphering keys are different.

20

22 (original): The method of claim 20, wherein the cryptography algorithm is
an asymmetric encryption-and-decryption algorithm such that an
enciphering key is not equal to the corresponding deciphering key,
and when a plaintext is enciphered into a ciphertext according to
25 the enciphering key by the cryptography algorithm, the
cryptography algorithm cannot decipher the ciphertext into the
original plaintext according to the enciphering key.

23 (cancelled)
30

24 (original): The method of claim 20 in which the communication device is a cell phone, and the communication network is a wireless communication network.